REMARKS

The Office Action dated March 5, 2004 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1-13 have been amended to more particularly point out and distinctly claim the subject matter of the present invention, and to correct informalities. Claims 14-21 are added. No new matter has been added. Because the amendments are not made in response to a statutory rejection, applicant submits that the pending claims are entitled to their full range of equivalents. Thus, claims 1-21 are pending in the present application and are respectfully submitted for consideration.

Claim 1 was objected to because of informalities. Applicant has amended the claims to correct the informalities. Thus, the objection is rendered moot.

Claims 1-13 were rejected under 35 U.S.C. §102(e) as allegedly being anticipated by U.S. Patent No. 5,991,407 (*Murto*). To anticipate, the cited reference must disclose each and every element of the claims. The Office Action took the position that *Murto* discloses all the features of independent claims 1 and 10. Applicant respectfully traverses the rejection and submits the presently pending claims are not disclosed or suggested by *Murto*.

Claim 1, upon which claims 2-9 depend, recites an authentication method for a telecommunications network. The method includes the step of transmitting from a terminal to the network an authenticator and a data unit containing information relating to

a manner in which the authenticator is formed. The method also includes the step of, in the network, determining a check value by means of the data unit, wherein the check value is compared with the authenticator. The method also includes the step of using an identification unit in the terminal of the network which receives a challenge as input from which it is possible to determine a response and a key essentially in the same way as in a subscriber identification module of a known mobile communications system.

The method also includes generating a set of subscriber-specific authentication data blocks into the network, each data block containing a challenge, a response and a key, whereby the generation is performed in the same manner as in the mobile communications system. The method also includes the step of transmitting at least some of the challenges contained in the authentication data blocks to the terminal. The method also includes choosing one of the challenges for use in the terminal, and based on the challenge, determining a response and a key to be used with an aid of the subscriber identity module of the terminal. The method also includes the step of notifying the network with the aid of the data unit of which keys corresponding to which challenge was chosen. The method also includes the step of determining the authenticator and the check value with the aid of the chosen key.

Claim 10, upon which claims 11-13 depend, recites an authentication system for a telecommunications network. The system includes in a terminal of the network, first message transmission means for transmitting an authenticator and a data unit to the network, the data unit including information relating to a manner in which the

authenticator is formed. The system also includes checking means for determining a check value with aid of the data unit. The system also includes the terminal of the network including such an identification unit, which receives as input a challenge from which a response and a key is defined essentially in a same manner as in a subscriber identity module of a known mobile communications system.

The system includes generating means for generating authentication data blocks in the same manner as in the mobile communications system, the authentication data blocks include a challenge, a response and a key. The system also includes transmission means for transmitting challenges contained by the authentication data blocks to the terminal, and the terminal includes selection means for selecting one challenge for use. The first message transmission means inserts such a value into the data unit which indicates which key corresponding to which challenge was selected for use in the terminal. The first message transmission means determines the authenticator and the checking means determine the check value based on the selected key.

As discussed in the specification, the present invention enables the use of a known authentication method of a telecommunications network for producing an authenticator for a terminal. A set of subscriber-specific authentication data blocks is generated in the network, such that each data block includes a challenge, response and key. The present invention enables a terminal to receive a challenge and determine a corresponding key and response. The response is sent from the terminal to the network, where the response received from the terminal is compared to the response calculated in the network. If

these two responses are equal, the terminal is successfully authenticated. Thus, it is possible to share a secret key between the terminal and the network for calculating an authenticator in the in the terminal and for checking the authenticator network. The authenticator may be calculated using any method, which has been, for example, agreed upon beforehand. For example, the authenticator may be an authenticator for a Mobile IP protocol. It is respectfully submitted that the prior art of *Murto* fails to disclose or suggest the elements of any of the presently pending claims. Therefore, the prior art fails to provide the critical and unobvious advantages discussed above.

Murto relates to subscriber authentication in a mobile communications system. *Murto* describes using one known authentication mechanism in a telecommunications network. Specifically, *Murto* describes an authentication mechanism in a global system for a mobile communications network using A3/A8 algorithms for calculating the response and key from a received challenge. Figures 2-5 of *Murto*, and the accompanying text, describe the authentication mechanism. For example, Figure 5 shows a challenge sent to the terminal and the terminal sending an authentication result to the network. *Murto* also describes using a CAVE authentication protocol in a global system for a mobile communications network. Because the input and output parameters of the CAVE and A3/A8 algorithms are different and have different lengths, *Murto* describes a solution for replacing A3/A8 algorithms with the CAVE algorithms, as shown in Figures 6 and 7.

Further, *Murto* describes a mobile station that receives an authentication request and extracts the challenge random number from the message. The mobile station of *Murto* performs computing, as shown in Figure 7, using a key corresponding to the challenge random number. The result of the computing is a response corresponding to the challenge. The terminal determines the response corresponding to the challenge, and sends the response to the network. Thus, only one challenge is sent at a time according to *Murto*. *Murto*, however, does not disclose or suggest transmitting at least some of the challenges contained in the authentication data blocks to the terminal, choosing one of the challenges for use in the terminal, and based on the challenge, determining a response and a key to be used with an aid of the subscriber identity module of the terminal.

In contrast, claim 1 recites "transmitting at least some of the challenges contained in the authentication data blocks to the terminal" and "choosing one of the challenges for use in the terminal, and based on the challenge, determining a response and a key to be used with an aid of the subscriber identity of the terminal." Claim 10 recites "the system includes transmission means for transmitting challenges contained by the authentication data blocks to the terminal and the terminal includes selection means for selecting one challenge for use." Further, applicant submits that *Murto* also does not disclose or suggest notifying the network with the aid of the data unit of which key corresponding to which challenge was chosen and determining the authenticator and the check value with the aid of the chosen key.

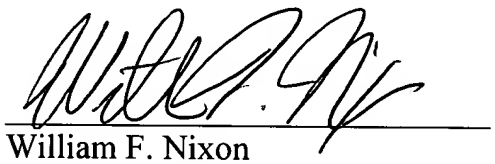
Thus, according to the claimed invention, at least some challenges are sent from the network to a terminal. The terminal chooses one of the challenges and determines a response and a key corresponding to the chosen challenge. The terminal determines an authenticator with the aid of the key corresponding to the chosen challenge and sends the authenticator to the network. The network should know which key the terminal used for the authenticator for determining a check value for the authenticator, and therefore the terminal notifies the network which challenged of the challenge chosen with the aid of a data unit. *Murto* does not disclose or suggest at least these features of the claimed invention. Applicant submits that *Murto* does not disclose or suggest sending a set of challenges to the terminal so that the terminal chooses one of the challenges, and, based on the challenge, determining a response and a key to be used with an aid of the subscriber identity module of the terminal. Thus, *Murto* does not disclose or suggest all the features of claims 1 and 10, and those claims depending therefrom. Applicant respectfully requests that the anticipation rejection of claims 1-13 be withdrawn.

Applicant submits new claims 14-21 that recite subject matter similar to claims 1-13 discussed above. Therefore, applicant submits that new claims 14-21 are allowable for at least the reasons given above. Further, it is submitted that all of the presently pending claims 1-21 recite subject matter that is neither disclosed nor suggested in the cited prior art. It is therefore respectfully requested that claims 1-21 be allowed, and this application passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, the applicant's undersigned attorney at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



William F. Nixon
Registration No. 44,262

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Tysons Corner, Virginia 22182-2700
Telephone: 703-720-7800
Fax: 703-720-7802

WFN:cct

Enclosures: Additional Claim Fee Transmittal